JOURNAL OF NUMBER THEORY **60**, 233–244 (1996)
ARTICLE NO. 0121

On Exponential Sums with Sparse Polynomials and Rational Functions

IGOR SHPARLINSKI*

School of MPCE, Macquarie University, Sydney, New South Wales 2109, Australia

Communicated by Alan C. Woods

Received December 2, 1994; revised June 19, 1995

INTRODUCTION

In this paper we obtain new upper bounds for exponential sums with polynomials of the form

$$f(x) = a_1 x^{r_1} + \cdots + a_t x^{r_t} \tag{1}$$

where $r_1, ..., r_t$ are some pairwise distinct non zero integers.

Throughout the paper:

$r = \max\{|r_1|, \ldots |r_t|\}$;

$(l_1, ..., l_m)$ denotes the greatest common divisor of $l_1, ..., l_m$;

for p prime, $\operatorname{ord}_p a$ denotes the p-adic order of a.

In the first part we consider rational exponential sums,

$$S(f, q) = \sum_{\substack{x=1 \\ (x, q)=1}}^{q} \exp\left[2\pi i f(x)/q\right]$$

* E-mail: igor@mpce.mg.edu.au.

0022-314X/96 $18.00

where q is integer, and prove that if $(a_1, ..., a_t, q) = 1$ then

$$S(f, q) = O(q^{1-1/t+\varepsilon}) \tag{2}$$

where the implied constant depends on r and an arbitrary $\varepsilon > 0$ only.

In the particular case when $q = p^\alpha$ is a power of a fixed prime number $p \geqslant 3$ (i.e. when the implied constant may depend on p), this bound is a direct consequence of the proved in [5] bound for exponential sums with linear recurrence sequences.

More precisely, let $U = \{u(z)\}_{z=1}^{\infty}$ be a non zero linear recurrence sequence of integers satisfying the following relation

$$u(z+t) = c_1 u(z+t-1) + \cdots + c_t u(z), \qquad z = 1, 2, ...,$$

of order t. Let $\lambda_1, ..., \lambda_t$ be the roots of the characteristic polynomial

$$\psi(\lambda) = \lambda^t - c_1 \lambda^{t-1} - \cdots - c_t \in \mathbb{Z}[\lambda].$$

If among λ_i and λ_i/λ_j, $1 \leqslant i, j \leqslant t$, $i \neq j$, there is no root of unity then

$$\sum_{z=1}^{\tau_\alpha} \exp[2\pi i u(z)/p^\alpha] \leqslant C(U, p, \varepsilon)\, \tau_\alpha^{1-1/t+\varepsilon}$$

where τ_α is the period U modulo p^α, and the constant $C(U, p, \varepsilon)$ depends on the sequence U, prime $p \geqslant 3$ and an arbitrary $\varepsilon > 0$.

Perhaps the same estimate can be proved for $p = 2$ as well. Moreover, using some results of [4] one can get it with $\varepsilon = 0$ (see also the remark after Theorem 1).

Substituting $x = g^z$ where g is a primitive root modulo p^2 (any thus modulo any power of $p \geqslant 3$) the sum $S(f, q)$ can be reduced to a sum with a linear recurrence sequence of order t and the above mentioned bound implies (2) for $q = p^\alpha$ with $p \geqslant 3$ fixed.

Here we use a modification of the method of [5] which allows us to prove (2) for any q.

We note that even in the most popular case of $r_1 = 1, ..., r_t = t$ (thus $r = t$) nothing essentially better than (2) is known (see [2, 3] for details). Of course we can apply the corresponding bound (at least if all $r_1, ..., r_t$ are positive) to our case as well but it gives only

$$S(f, q) = O(q^{1-1/r+\varepsilon}).$$

In the second part we consider sums

$$T_m(f) = \sum_{x \in \mathbb{F}_{2^m}} \chi(f(x))$$

where χ is a non trivial additive character of $\mathbb{F}_{2^m}$, a field of 2^m elements.

For such sums, we have the following very deep and strong Weil bound

$$T_m(f) \leqslant r2^{m/2}$$

(see [3] and [10] for this and many other related results). However, our bound is better if r large enough (in particular, when $r \geqslant 2^{m/2}$, the Weil bound gives nothing but ours is still non trivial).

The proposed method is a generalization of those of the papers [6–9] devoted to estimating Gaussian sums (i.e. to the case $t = 1$) and parameters of cyclic linear codes. it can be easily extended to arbitrary finite fields of fixed characteristic.

The obtained upper bound is non trivial for a wide range of parameters and provides a new asymptotic formula for the number of solutions of the system of equations

$$x_1^{r_i} + \cdots + x_k^{r_i} = A_i, \qquad i = 1, ..., t; \qquad x_1, \ldots x_k \in \mathbb{F}_{2^m}. \tag{3}$$

For instance, we derive an upper bound for $k(r_1, ..., r_t; m)$, that is the smallest k such tat the system (3) is solvable for any $A_1, ..., A_t \in \mathbb{F}_{2^m}$. This result can be reformulated as a result on the covering radius of certain cyclic linear codes (see [1]).

1. Rational Exponential Sums

In this section all implied constants depends on r and an arbitrary $\varepsilon > 0$ only. Denote by $\Delta(r_1, ..., r_t)$ the following determinant

$$\Delta(r_1, ..., r_t) = \det \begin{pmatrix} \binom{r_1}{1}, & ..., & \binom{r_t}{1} \\ ..., & ..., & ... \\ \binom{r_1}{t}, & ..., & \binom{r_t}{t} \end{pmatrix},$$

where for integers $m \geqslant 0$ and k we set

$$\binom{k}{m} = \frac{k(k-1)\cdots(k-m+1)}{m!}.$$

Lemma 1. *We have*

$$0 < |\Delta(r_1, ..., r_t)| \leqslant (3r)^{t(t+1)}.$$

Proof. We have

$$\binom{r_v}{i} \leqslant (r+t)^i \leqslant (3r)^i, \qquad 1 \leqslant i, v \leqslant t,$$

thus

$$|\Delta(r_1, ..., r_t)| \leqslant t!(3r)^{t(t+1)/2} \leqslant (3rt)^{t(t+1)/2} \leqslant (6r^2)^{t(t+1)/2} \leqslant (3r)^{t(t+1)}.$$

Now we show that

$$\Delta(r_1, ..., r_t) \neq 0.$$

Indeed, otherwise there exist some integers $c_1, ..., c_t$, not all equal to zero and such that

$$\sum_{i=1}^{t} \frac{c_i}{i!} \prod_{j=1}^{i} (r_v - j + 1) = 0, \qquad 1 \leqslant v \leqslant t.$$

Then the polynomial

$$R(x) = \sum_{i=1}^{t} \frac{c_i}{i!} \prod_{j=1}^{i} (x - j + 1)$$

is of degree $\deg R \leqslant t < p$ and has at least $t+1$ distinct roots $0, r_1, ..., r_t$. Thus it must be identical to zero that contradicts to the assumption that $c_1, ..., c_t$ are not all equal to zero. ∎

It is clear that one can get a much sharper bound of $|\Delta(r_1, ..., r_t)|$ (it would really make sense in case we were going to evaluate the implied constants explicitly).

Let us define the following differential operators

$$D = \left(\frac{d}{dx}\right), \qquad D_v = (v!)^{-1}, \qquad v = 0, 1, ...$$

LEMMA 2. *Let p be a prime with $(p, a_1, ..., a_t) = 1$, then for $(x, p) = 1$,*

$$\operatorname{ord}_p(D_1 f(x), ..., D_t f(x)) \leqslant \operatorname{ord}_p \Delta(r_1, ..., r_t)$$

Proof. We set

$$\theta = \operatorname{ord}_p (D_1 f(x), ..., D_t f(x)).$$

Then we have

$$a_1 \binom{r_1}{v} x^{r_1 - v} + \cdots + a_t \binom{r_t}{v} x^{r_t - v} \equiv 0 \pmod{p^\theta}, \qquad v = 1, ..., t.$$

Multiplying the v-th congruence by x^v we obtain the system of congruences

$$\xi_1 \binom{r_1}{v} + \cdots + \xi_t \binom{r_t}{v} \equiv 0 \pmod{p^\theta}, \qquad v = 1, ..., t$$

which has a non zero modulo p solution, namely $\xi_1 = a_1 x^{r_1}, ..., \xi_t = a_t x^{r_t}$. Therefore the determinant $\Delta(r_1, ..., r_t)$ of the system is divisible by p^θ. ∎

LEMMA 3. *Let integer positive α, β, m satisfying the inequalities*

$$\beta m < \alpha \leqslant \beta(m+1).$$

Then for any integer x and y with $(x, p) = 1$ we have

$$f(x + p^\beta y) \equiv \sum_{v=0}^{m} p^{\beta v} y^v D_v f(x) \pmod{p^\alpha}.$$

Proof. Define integers s_i from the following conditions

$$r_i \equiv s_i \pmod{p^{\alpha-1}(p-1)}, \qquad 0 \leqslant s_i \leqslant p^{\alpha-1}(p-1)$$

and define

$$F(x) = a_1 x^{s_1} + \cdots + a_t x^{s_t}.$$

It is evident that $f(x) \equiv F(x) \pmod{p^\alpha}$ and

$$D_v f(x) \equiv D_v F(x) \pmod{p^{\alpha-1}}, \qquad v = 1, 2, ...,$$

for $(x, p) = 1$. Let $s = \max\{s_1, ..., s_t\}$ be the degree of F. Then

$$\begin{aligned} f(x + p^\beta y) \equiv F(x + p^\beta y) &\equiv \sum_{v=0}^{s} p^{\beta v} y^v D_v F(x) \\ &\equiv \sum_{v=0}^{m} p^{\beta v} y^v D_v F(x) \equiv \sum_{v=0}^{m} p^{\beta v} y^v D_v f(x) \pmod{p^\alpha} \end{aligned}$$

and the lemma is proved. ∎

LEMMA 4. *Let p be a prime and let*

$$F(y) = p^{\gamma} H(y)\, y^{h+1} + G(y)$$

where $H(y), G(y) \in \mathbb{Z}[y]$, γ and h are integer positive with

$$\gamma > \log h / \log p.$$

Assume that at least one coefficient of $G(y)$ is not divisible by p, then for any $\mu \geqslant 1$ if $h \geqslant 2$ and for any $\mu \geqslant 2$ if $h = 1$ the bound

$$\left| \sum_{y=1}^{p^{\mu}} \exp\left[2\pi i F(y)/p^{\mu}\right] \right| \leqslant 2h^{5/2} p^{\mu(1-1/h)}$$

holds.

Proof. This is Corollary of Lemma 1.2 of [4]. ∎

LEMMA 5. *Let p be a prime with $(p, a_1, ..., a_t) = 1$ and let $t \geqslant 2$. Then for any integer $\alpha > 0$,*

$$S(f, p^{\alpha}) = O(p^{\alpha(1-1/t+\varepsilon)}).$$

Proof. Set $\rho = \operatorname{ord}_p \Delta(r_1, ..., r_t)$. It follows from Lemma 1 that

$$p^{\rho} \leqslant (3r)^{t(t+1)}. \tag{4}$$

First of all we note that for $\alpha = 1$ the bound of the lemma is weaker than the Weil bound

$$|S(f, p)| = O(p^{1/2})$$

and that for $\alpha \leqslant \varepsilon^{-1}(\rho + \log t/\log p)$

$$|S(f, p^{\alpha})| \leqslant p^{\alpha} \leqslant (tp^{\rho})^{\varepsilon^{-1}} \leqslant (t(3r)^{t(t+1)})^{\varepsilon^{-1}} = O(1).$$

Thus we may assume that

$$\alpha > \max\{1, \varepsilon^{-1}(\rho + \log t/\log p)\} \tag{5}$$

and that $\varepsilon < 1/t$. Set $\beta = \lfloor \varepsilon\alpha \rfloor + 1$ and define m from inequalities

$$\beta m < \alpha \leqslant \beta(m+1).$$

We have $\varepsilon\alpha < \beta < \alpha/2 + 1 \leqslant \alpha$ hence $1 \leqslant m < \varepsilon^{-1} = O(1)$. Now, from Lemma 3 we obtain

$$S(f, p^\alpha) = \sum_{\substack{x=1 \\ (x,p)=1}}^{p^\beta} \sum_{y=1}^{p^{\alpha-\beta}} \exp\left[2\pi i f(x + p^\beta y)/p^\alpha\right] = \sum_{\substack{x=1 \\ (x,p)=1}}^{p^\beta} \sigma(x) \exp\left[2\pi i f(x)/p^\alpha\right] \tag{6}$$

where

$$\sigma(x) = \sum_{y=1}^{p^{\alpha-\beta}} \exp\left[2\pi i \left(\sum_{v=1}^{m} p^{\beta(v-1)} y^v D_v f(x)\right) \Big/ p^{\alpha-\beta}\right].$$

We show that if $Df(x) \not\equiv 0 \pmod p$ then

$$\sigma(x) = O(p^{\alpha(1-1/t)-1}). \tag{7}$$

We consider three possibilities.

If $\alpha - \beta > 1$ (and therefore $\alpha \geqslant \beta + 2 \geqslant 3$) then we use Lemma 4 with $\gamma = \beta$ and $h = 1$; it gives $\sigma(x) = O(1)$ (in fact, one can easily prove that $\sigma(x) = 0$ in this case).

If $\alpha = 2$, $\beta = 1$ then $m = 1$ and $\sigma(x) = 0$.

If $\alpha - \beta = 1$ and $\alpha \geqslant 3$ then we use the Weil bound; it gives $\sigma(x) = O(p^{1/2})$.

In the second case there is nothing to prove. In the first and third cases, since $\alpha \geqslant 3$ we have $\alpha(1-1/t) - 1 \geqslant 3/2 - 1 \geqslant 1/2 \geqslant 0$ and the bound (7) follows.

Now we show that for any x with $(x, p) = 1$ the bound

$$\sigma(x) = O(p^{\alpha(1-1/t)}). \tag{8}$$

holds. If $m < t$ then $\alpha \leqslant \beta t$ and

$$|\sigma(x)| = p^{\alpha-\beta} \leqslant p^{\alpha(1-1/t)}.$$

Therefore we may assume that $m \geqslant t$. We define

$$\theta = \operatorname{ord}_p(D_1 f(x), p^\beta D_2 f(x), \ldots, p^{\beta(t-1)} D_t f(x)).$$

It follows from Lemma 2 that

$$\theta \leqslant \rho + \beta(t-1).$$

Hence, from (5) we get

$$\beta t - \theta \geqslant \beta - \rho > \varepsilon\alpha - \rho \geqslant \log t/\log p.$$

If $\theta \geqslant \alpha - \beta$ then, recalling that $\alpha > m\beta \geqslant t\beta$ and the inequality (4), we obtain

$$|\sigma(x)| \leqslant p^{\alpha-\beta} \leqslant p^{\theta} \leqslant p^{\rho+\beta(t-1)} \leqslant p^{\rho} p^{\alpha(t-1)/t} = O(p^{\alpha(1-1/t)}).$$

Finally, if $\theta < \alpha - \beta$ then we have the representation

$$\sum_{v=1}^{m} p^{\beta(v-1)} y^{v} D_v f(x) = p^{\theta}(p^{\beta t-\theta} H_x(y)\, y^{t+1} + G_x(y))$$

where the polynomial

$$F_x(y) = p^{\beta t-\theta} H_x(y)\, y^{t+1} + G_x(y)$$

satisfies the condition of Lemma 4 with

$$\gamma = \beta t - \theta > \log t/\log p, \qquad h = t \geqslant 2.$$

Applying the bound of that lemma with $\mu = \alpha - \beta - \theta \geqslant 1$ we get

$$\sigma(x) = p^{\theta} \sum_{y=1}^{p^{\alpha-\beta-\theta}} \exp\,[2\pi i F_x(y)/p^{\alpha-\beta-\theta}] = O(p^{\theta+(\alpha-\beta-\theta)(1-1/t)}).$$

Furthermore, we have

$$\theta + (\alpha-\beta-\theta)(1-1/t) = \theta/t + (\alpha-\beta)(1-1/t) \leqslant \rho/t + \alpha(1-1/t).$$

From this inequality and from (4) we obtain (8).

Evidently, for $x = 1, ..., p^{\beta}$ the congruence $Df(x) \equiv 0 \pmod p$ has at most $2rp^{\beta-1}$ solutions. We shall apply the estimate (8) to such x and the estimate (7) to other $x = 1, ..., p^{\beta}$, $(x, p) = 1$. The contribution to (6) of sums $\sigma(x)$ over x of either kind is $p^{\beta+\alpha(1-1/t)-1}$. Taking into account that $\beta \leqslant \varepsilon\alpha + 1$ we obtain the assertion. ∎

The following statement is Problem 11.d of Chapter 3 of [11].

LEMMA 6. *Let $q = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the prime number factorization of integer q. Then*

$$S(f, q) = \prod_{v=1}^{s} S(f_v, p_v^{\alpha_v})$$

where

$$f_v(x) \equiv q_v^{-1} f(q_v x) \pmod{p_v^{\alpha_v}}$$

and $q_v = q/p_v^{\alpha_v}$, $v = 1, ..., s$.

THEOREM 1. *Let* $q \geqslant 1$ *and* $t \geqslant 2$ *be integer and let* f *be a rational function given by* (1) *with pairwise distinct non zero integers* $r_1, ..., r_t$. *Assume that* $(q, a_1, ..., a_t) = 1$, *then for any* $\varepsilon > 0$ *the bound*

$$S(f, q) = O(q^{1-1/t+\varepsilon})$$

holds.

Proof. From Lemma 5 (applied with $\varepsilon/2$ rather than with ε) and Lemma 6 we obtain that there is some constant $C > O$ depending on ε and such that

$$S(f, q) \leqslant C^s q^{1-1/t+\varepsilon/2}.$$

Evidently, $s! \leqslant q$ thus $s = O(\log q/\log\log q)$. It implies $C^s = O(q^{\varepsilon/2})$ and the theorem follows. ∎

Note that Lemma 5 perhaps can be proved with $\varepsilon = 0$ as well but it is not clear at all if it can be done for Theorem 1. To obtain such a result one has to prove that the implied constant in the bound of Lemma 5 equals 1 for sufficiently large p.

2. EXPONENTIAL SUMS OVER $\mathbb{F}_{2^m}$

For $0 < \lambda < 1$ let us denote by $\theta(\lambda)$ the root of the equation

$$\theta \log_2 \theta + (1-\theta)\log_2(1-\theta) = -\lambda, \qquad 0 < \theta < 1/2$$

(it is easy to see that this equation has a unique root for any $0 < \lambda < 1$).

Set $\gamma(\lambda) = 1 - 2\theta(\lambda)$.

THEOREM 2. *Let* $0 < \alpha < 1$ *be a fixed real number and let the exponents* $r_1, ..., r_t$ *satisfy*

$$r_i 2^k \not\equiv r_j \pmod{2^m - 1},$$

$1 \leqslant i < j \leqslant t$, $k = 0, 1, ..., m$. *Assume that*

$$(2^m - 1, r_1, ..., r_t) < 2^{\alpha m},$$

then for any rational function f given by (1) *with* $a_1, ..., a_t \in \mathbb{F}_{2^m}^*$ *the bound*

$$T_m(f) < \gamma((1-\alpha)/t)\, 2^m + o(2^m), \qquad m \to \infty,$$

holds.

Proof. It is known that any non principal additive character χ of $\mathbb{F}_{2^m}$ can be represented in the form

$$\chi(\lambda) = (-1)^{\mathrm{Tr}(a\lambda)}$$

with some $a \in \mathbb{F}_{2^m}^*$, where $\mathrm{Tr}(\mu)$ is the trace of $\mu \in \mathbb{F}_{2^m}$ in $\mathbb{F}_2$.

Let g be a primitive root of $\mathbb{F}_{2^m}$, then

$$T_m(f) = 1 + \sum_{z=1}^{2^m-1} (-1)^{u(z)}$$

where

$$u(z) = \mathrm{Tr}\left(a \sum_{i=1}^{t} a_i g^{r_i z}\right).$$

We put, $b_i = aa_i$, $i = 1, ..., t$, then

$$u(z) = \sum_{k=0}^{m-1} \sum_{i=1}^{t} b_i^{2^k} g^{2^k r_i z}. \tag{9}$$

Evidently, $u(x)$ is a linear recurrence sequence of order $N = mt$, which is the number of pairwise distinct exponential functions in the representation (9).

Let τ be the period of this sequence, i.e. the minimal integer positive number with $u(z+\tau) = u(z)$, $z = 1, 2, ...$ Then from (9) we obtain

$$\sum_{k=0}^{m-1} \sum_{i=1}^{t} b_i^{2^k} g^{2^k r_i z} (g^{2^k r_i \tau} - 1) = 0, \qquad z = 1, 2, ... \tag{10}$$

Since the exponents $2^k r_i$, $k = 0, ..., m-1$, $i = 1, ..., t$, are pairwise distinct modulo $2^m - 1$, the identity (10) holds for all integer $z \geqslant 1$ if and only if

$$g^{2^k r_i \tau} - 1 = 0, \qquad k = 0, ..., m-1, \quad i = 1, ..., t.$$

These equations are equivalent to

$$2^k r_i \tau \equiv 0 \pmod{2^m - 1}, \qquad k = 0, ..., m-1, \quad i = 1, ..., t,$$

or just

$$r_i \tau \equiv 0 \pmod{2^m - 1}, \qquad i = 1, ..., t.$$

Hence

$$\tau = \frac{2^m - 1}{(2^m - 1, r_1, ..., r_t)}.$$

The condition of the theorem infers

$$\tau \geqslant (2^m - 1)\, 2^{-\alpha m}.$$

It is easy to see that

$$T_m(f) = 1 + \frac{2^m - 1}{\tau} \sum_{z=1}^{\tau} (-1)^{u(z)} = 1 + \frac{2^m - 1}{\tau} (N_0 - N_1),$$

where N_0 and N_1 are the numbers of solutions of the equations $u(z) = 0$, $1 \leqslant z \leqslant \tau$, and $u(z) = 1$, $1 \leqslant z \leqslant \tau$, respectively.

Theorem 2 of [6] asserts that

$$N_1 \geqslant \theta(\log_2 \tau / N)\, \tau + o(\tau) = \theta((1 - \alpha)/t)\, \tau + o(\tau).$$

Applying the same result to the sequence $v(z) = 1 - u(z)$ we get

$$N_0 \geqslant \theta((1 - \alpha)/t)\, \tau + o(\tau).$$

Taking into account that $N_0 + N_1 = \tau$ we obtain

$$N_0 = \tau - N_1 \leqslant \tau - \theta(\log_2 \tau / N)\, \tau + o(\tau) = \tau - \theta((1 - \alpha)/t)\, \tau + o(\tau),$$

$$|N_0 - N_1| = |2N_0 - \tau| \leqslant \tau - 2\theta((1 - \alpha)/t)\, \tau + o(\tau)$$

and the bound follows. ∎

Denote by $k(r_1, ..., r_t; m)$ the smallest k for which the system (3) is solvable for any $A_1, ..., A_t \in \mathbb{F}_{2^m}$.

COROLLARY. *Let $0 < \alpha < 1$ be a fixed real number and let the exponents $r_1, ..., r_t$ satisfy*

$$r_i\, 2^k \not\equiv r_j \pmod{2^m - 1},$$

$1 \leqslant i < j \leqslant t$, $k = 0, 1, ..., m$. Assume also that

$$(2^m - 1, r_i) < 2^{\alpha m}, \qquad i = 1, ..., t.$$

Then there is a constant $C > 0$ depending on α and such that the bound

$$k(r_1, ..., r_t; m) \leqslant Cmt^2 \log(t + 1)$$

holds.

Proof. It is clear that we may assume that m is large enough.

Let N be the number of solutions of the system (3). Then, using the standard arguments (as it has been done in [1], for example), for a non trivial additive character χ of $\mathbb{F}_{2^m}$, we obtain

$$N = 2^{-mt} \sum_{a_1, \ldots, a_t \in \mathbb{F}_{2^m}} \chi(-a_1 A_1 - \cdots - a_t A_t) \left(\sum_{x \in \mathbb{F}_{2^m}} \chi(a_1 x^{r_1} + \ldots + a_t x^{r_t}) \right)^k.$$

Separating the term corresponding to $a_1 = \cdots = a_t = 0$ and applying the bound of Theorem 2 to other terms, we get

$$N = 2^{mk - mt} + O(\gamma^k((1-\alpha)/t)\, 2^{mk}).$$

From the definition of $\theta(\lambda)$, one gets $\theta(\lambda) \sim \lambda/\log_2 \lambda$ if $\lambda \to 0$. Thus there exists a constant $A > 0$ depending on α and such that

$$\gamma((1-\alpha)/t) \leqslant 1 - A/t \log(t+1).$$

Hence there are some positive constants B and C depending on α and such that for $k \geqslant Cmt^2 \log(t+1) - 1$ we have

$$\gamma^k((1-\alpha)/t) \leqslant (1 - A/t \log(t+1))^k \leqslant \exp(-Bk/t \log(t+1)) < 2^{-2mt}.$$

Therefore $N > 0$ for some $k \geqslant Cmt^2 \log(t+1)$. ∎

References

1. T. Helleseth, On the covering radius of cyclic linear codes and arithmetical codes, *Discr. Appl. Math.* **11** (1985), 157–173.
2. L.-K. Hua, "Abschätzungen von Exponentialsummen und ihre Anwendung in der Zahlentheorie," Teubner-Verlag, Leipzig, 1959.
3. R. Lidl and H. Niederreiter, "Finite Fields," Addison–Wesley, 1983.
4. D. A. Mit'kin, Estimates and asymptotic formulas for rational exponential sums that are nearly complete, *Matem. Sborn.* **122**, No. 4 (1983), 527–545. [Russian]
5. I. Shparlinski, Bounds for exponential sums with recurrence sequences and their applications, *Proc. Voronezh State Pedagog. Inst.* **197** (1978), 74–85. [Russian]
6. I. Shparlinski, On some properties of linear cyclic codes, *Problemy Peredachi Inform.* **19**, No. 3 (1983), 106–110. [Russian]
7. I. Shparlinski, On weight spectra of some codes, *Probl. Peredachi Inform.* **22**, No. 2 (1986), 43–48. [Russian]
8. I. Shparlinski, On bounds of Gaussian sums, *Mat. Zametki* **50**, No. 1 (1991), 122–130. [Russian]
9. I. Shparlinski, On Gaussian sums for finite fields and elliptic curves, *Lect. Notes Comp. Sci.* **573** (1992), 5–15.
10. I. Shparlinski, "Computational and Algorithmic Problems in Finite Fields," Kluwer Acad., The Netherlands, 1992.
11. I. M. Vinogradov, "Basics of number theory," Nauka, Moscow, 1981. [Russian]